Théorie des groupes

Feuille de TD n° 11

Exercice 1 Montrer qu'un groupe d'ordre pq (avec p et q deux entiers premiers distincts) n'est pas simple.

Exercice 2 Montrer qu'un groupe d'ordre p^2q n'est pas simple (attention au cas $p = 2$ et $q = 3$).

Exercice 3 Montrer qu'un groupe d'ordre p^2q^2 n'est jamais simple (attention au cas $p = 2$ et $q = 3$).

Exercice 4 Soit G un groupe d'ordre pqr (avec $p > q > r$ trois entiers premiers).
Montrer que $pqr \geq n_p(p-1) + n_q(q-1) + n_r(r-1) + 1$ et en déduire que G n'est jamais simple.

Exercice 5

1. Montrer que si $|G| \in \{24, 40, 48, 56\}$ alors G n'est pas simple (si besoin, faire agir G sur un ensembles de Sylows).
2. Déduire de la question précédente et des exercices 1, 2, 3 et 4 qu'un groupe G d'ordre $|G| < 60$ simple est alors cyclique d'ordre p premier.

Exercice 6 Soit G un groupe simple d'ordre $60 = 2^2 \cdot 3 \cdot 5$.

1. Montrer que les nombres de sous-groupes de Sylow vérifient
$$n_5 = 6, \quad n_3 \in \{4, 10\} \quad \text{et} \quad n_2 \in \{3, 5, 15\}.$$
2. En faisant agir G sur l'ensemble des 3-Sylows, montrer que $n_3 = 4$ est exclue. De même, montrer que $n_2 = 3$ ne peut survenir.
3. Si $n_2 = 5$, faire agir G sur les 2-Sylows et montrer que $G \simeq \mathsf{A}_5$ (on vérifiera que A_5 a bien les caractéristiques suivantes : $n_2(\mathsf{A}_5) = 5$, $n_3(\mathsf{A}_5) = 10$ et $n_5(\mathsf{A}_5) = 6$).
4. Par un argument de comptage, montrer que, si $n_2 = 15$, alors il existe S_1 et S_2 des 2-Sylows vérifiant $S_1 \cap S_2 = \{1, g\}$. Montrer que le centralisateur de g a pour ordre $|C_G(g)| = 12$ ou 20 et aboutir à une contradiction.

TD Théorie des groupes

Mercedes Haiech

7 décembre 2021

Table des matières

1 TD11

Théorème 1.1 (Théorème de Sylow (rappel))**.** *Soit G un groupe de cardinal $|G| = p^\alpha m$ avec p premier qui ne divise pas m.*

1. *Si H est un p-sous-groupe de G, alors il existe un p-Sylow S tel que $H \subset S$.*
2. *Les p-Sylow sont tous conjugués et leur nombre n_p divise n.*
3. *On a $n_p \equiv 1 \mod (p)$, donc k divise m.*

1.1 Exo 1

Exercice 1.1. Montrer qu'un groupe d'ordre pq (avec p et q deux entiers premiers distincts) n'est pas simple.

Démonstration. On suppose que $p > q$. D'après le théorème de Sylow, il existe un p-Sylow disons S et le nombre de p-Sylow divise q et est congru à 1 modulo p. En particulier $n_p \leqslant q < p$, et $n_p \equiv 1 \mod (p)$. Finalement le seul choix possible est $n_p = 1$.

Comme tous les p-Sylow sont conjugués et qu'il n'y en a qu'un, on en déduit que S est distingué, donc que le groupe n'est pas simple. □

1.2 Exo 2

Exercice 1.2. Montrer qu'un groupe d'ordre p^2q n'est pas simple (attention au cas $p = 2$ et $q = 3$).

Démonstration. On va traiter deux cas selon que $p > q$ ou que $q > p$.

• Si $p > q$, alors il existe un p-Sylow et le nombre n_p de p-Sylow vérifie $n_p|q$ et $n_p \equiv 1 \mod (p)$. En particulier $n_p \leqslant q < p$, donc $n_p = 1$. Comme tous les p-Sylow sont conjugués, alors S est un sous-groupe distingué.

• Si $q > p$, alors il existe un q-Sylow S, et le nombre n_q de q-Sylow vérifie $n_q|p^2$ et $n_q \equiv 1 \mod (q)$. En particulier $n_q \in \{1, p, p^2\}$.

Si $n_q = p$ alors comme $q > p$, on aurait $p \equiv 1 \mod (q)$, ce qui est impossible. Si $n_q = p^2$, alors $p^2 \equiv 1 \mod (q)$, et donc $p \equiv 1 \mod (q)$ ou $p \equiv -1 \mod (q)$. Comme le premier cas est impossible, on a nécessairement $p \equiv -1 \mod (q)$, ce qui implique $p = q-1$. Or q étant impair, alors p est pair, ce qui n'est possible que si $p = 2$ et $q = 3$. Dans tous les autres cas, on a alors $n_q = 1$, et donc S est distingué.

Si jamais $p = 2$ et $q = 3$. Supposons que $n_3 \neq 1$, alors comme $n_3|4$ et $n_3 \equiv 1 \mod (3)$, on a $n_3 = 4$. Ainsi le groupe contient quatre 3-Sylow et leur union contient 8 éléments d'ordre 3 (et l'identité). Il ne reste alors de la place que pour un 2-Sylow, qui est alors unique et donc distingué. □

1.3 Exo 3

Exercice 1.3. Montrer qu'un groupe d'ordre p^2q^2 n'est jamais simple (attention au cas $p = 2$ et $q = 3$).

Démonstration. Par symétrie, on peut supposer sans perte de généralité que $p > q$. Il existe un p-Sylow, disons S et le nombre n_p de p-Sylow vérifie $n_p|q^2$ et $n_p \equiv 1 \mod (p)$. En particulier $n_q \in \{1, q, q^2\}$.

Si $n_p = q$ alors comme $p > q$, on aurait $q \equiv 1 \mod (p)$, ce qui est impossible.

Si $n_p = q^2$, alors $q^2 \equiv 1 \mod (p)$, et donc $q \equiv 1 \mod (p)$ ou $q \equiv -1 \mod (p)$. Comme le premier cas est impossible, on a nécessairement $q \equiv -1 \mod (p)$, ce qui implique $q = p - 1$. Or p étant impair, alors q est pair, ce qui n'est possible que si $q = 2$ et $p = 3$. Dans tous les autres cas, on a alors $n_p = 1$, et donc S est distingué.

Si jamais $p = 2$ et $q = 3$. Comme tous les 3-Sylow sont conjugués on peut définir une action de G sur l'ensemble de ses 3-Sylow. On sait que $n_3|4$ et $n_3 \equiv 1 \mod (3)$, alors

$n_3 = 1$ ou 4. Supposons que $n_3 = 4$. Cela induit un morphisme de groupe $\varphi\colon G \to \mathfrak{S}_4$. Or $4! = 24$ et $24 < 36$, donc φ ne peut pas être injectif et son noyau est un sous-groupe distingué non trivial. $\square$

1.4 Exo 4

Exercice 1.4. Montrer qu'un groupe d'ordre pqr (avec $p > q > r$ trois entiers premiers) n'est jamais simple.

Démonstration. Puisque $n_p | qr$ on a que $n_p \in \{1, q, r, qr\}$. Puisque $n_p \equiv 1 \mod (p)$, on ne peut pas avoir $n_p \in \{q, r\}$. Supposons que $n_p = qr$. Alors deux p-Sylow ont une intersection triviale (car engendrés par élément d'ordre p, et si leur intersection est non triviale alors ils sont égaux). Le groupe G contient alors $qr(p-1)$ éléments d'ordre p. Si en outre $n_r, n_q \neq 1$, alors comme $n_r | pq$ et $n_q | pr$, alors $n_r \geqslant q$ et $n_q \geqslant r$ et G contient au moins $q(r-1)+r(q-1)$ éléments d'ordre r ou q. Ainsi, en comptant le neutre pour G, on a :

$$qr(p-1) + q(r-1) + r(q-1) + 1 \leqslant |G| = pqr$$

En particulier, on a $q(r-1) + r(q-1) + 1 \leqslant qr$, soit encore $q + r \geqslant qr + 1$. Puisque $2 \leqslant r < q$, on a en particulier $2q + 1 \leqslant 2q$, ce qui est absurde.

Donc $n_p = qr$ donne $n_q = 1$ ou $n_r = 1$, dans tous les cas G possède un sous-groupe distingué. $\square$

1.5 Exo 5

Exercice 1.5.

1. Montrer que si $|G| \in \{24, 40, 48, 56\}$ alors G n'est pas simple (si besoin, faire agir G sur un ensembles de Sylows).
2. Déduire de la question précédente et des exercices 1.1, 1.2, 1.3 et 1.4 qu'un groupe G d'ordre $|G| < 60$ simple est alors cyclique d'ordre p premier.

Démonstration.

1. Si $|G| = 24$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2 | 3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 24$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué de G non trivial.
2. Si $|G| = 40 = 2^3 \times 5$. Alors $n_5 | 8$ et $n_5 \equiv 1 \mod (5)$. Donc $n_5 \in \{1, 2, 4, 8\}$. Or le seul élément de cet ensemble qui vérifie $n_5 \equiv 1 \mod (5)$ est 1. Donc $n_5 = 1$.
3. Si $|G| = 48 = 2^4 \times 3$ on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2 | 3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 48$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué de G non trivial.
4. Si $|G| = 56$ alors $n_7 | 8$ et $n_7 \equiv 1 \mod (7)$. Alors $n_7 \in \{1, 8\}$. Supposons que $n_7 = 8$. Alors deux 7-Sylow disjoints ont une intersection triviale et G possède $8 \times 6 = 48$ éléments d'ordre 7. Il reste donc $56 - 48 = 8$ autres éléments, soit juste assez de place pour un 2-Sylow qui est donc unique et distingué. Dans tous les cas, G n'est pas simple.
5. Soit G un groupe d'ordre < 60 non banal (pas un $\mathbf{F}_p$). Si p est premier et $\alpha > 1$, alors un groupe d'ordre p^α n'est pas simple car son centre n'est pas réduit au neutre (et tout sous-groupe du centre est distingué). Les exercices 1.1, 1.2, 1.3 et 1.4 nous assurent que tout groupe d'ordre pq, p^2q, p^2q^2 et pqr ne sont pas simple. Si jamais un groupe G a un facteur de type p^3q. Comme $3^3 \times 5 > 60$, les seules possibilités sont $|G| \in \{2^3 \times 3, 2^3 \times 5, 2^3 \times 7, 3^3 \times 2\}$. Mais $3^3 \times 2 = 54$ n'est pas simple (on fait comme dans l'exercice 1.1 en considérant les 3-Sylow) et on a vu que dans les autres possibilités G n'est pas simple. Si G a un facteur de type p^4q, alors comme $3^4 = 81 > 60$, et que $2^4 \times 5 = 80 > 60$, la seule possibilité est $|G| = 2^4 \times 3 = 48$. On

a vu qu'un tel groupe n'était pas simple. Comme $2^5 = 32$, on n'aura pas de groupe avec un facteur du type $p^5 q$.

On a couvert toutes les possibilités, donc un groupe G d'ordre $|G| < 60$ simple est alors cyclique d'ordre p premier.

$\square$

1.6 Exo 6

Exercice 1.6. Soit G un groupe simple d'ordre $60 = 2^2 \cdot 3 \cdot 5$.

1. Montrer que les nombres de sous-groupes de Sylow vérifient
$$s_5 = 6, \quad s_3 \in \{4,\ 10\} \quad \text{et} \quad s_2 \in \{3,\ 5,\ 15\}\,.$$
2. En faisant agir G sur l'ensemble des 3-Sylows, montrer que $s_3 = 4$ est exclue. De même, montrer que $s_2 = 3$ ne peut survenir.
3. Si $s_2 = 5$, faire agir G sur les 2-Sylows et montrer que $G \simeq \mathfrak{A}_5$ (on vérifiera que $\mathfrak{A}_5$ a bien les caractéristiques suivantes : $s_2(\mathfrak{A}_5) = 5$, $s_3(\mathfrak{A}_5) = 10$ et $s_5(\mathfrak{A}_5) = 6$).
4. Par un argument de comptage, montrer que, si $s_2 = 15$, alors il existe S_1 et S_2 des 2-Sylows vérifiant $S_1 \cap S_2 = \{1, g\}$. Montrer que le centralisateur de g a pour ordre $|C_G(g)| = 12$ ou 20 et aboutir à une contradiction.

Démonstration. On n'a jamais $s_k = 1$ sinon G ne serait pas distingué.

1. D'après le théorème de Sylow, on sait que $s_5 \in \{2,3,4,6,12\}$ et que $s_5 \equiv 1 \mod (5)$. Donc nécessairement $s_5 = 6$.

   De même $s_3 \in \{2,4,5,10,20\}$ et $s_3 \equiv 1 \mod (3)$, donc nécessairement $s_3 \in \{4,10\}$.

   De même $s_2 \in \{3,5,15\}$ et $s_3 \equiv 1 \mod (2)$, ce qui n'apporte aucune information supplémentaire.
2. Supposons par l'absurde que $s_3 = 4$, alors l'action de G sur ses 3-Sylow par conjugaison induit un morphisme $\rho\colon G \to \mathfrak{S}_4$. Pour des raisons de cardinalité, ce morphisme n'est pas injectif. Il n'est pas non plus trivial car tous les 3-Sylow sont conjugués. Cela implique que $\mathrm{Ker}(\rho)$ est un sous-groupe distingué non trivial de G, ce qui est impossible puisque G est simple.

   Les mêmes arguments en faisant agir G sur ses 2-Sylow prouve que $s_2 = 3$ est exclu.
3. Si $s_2 = 5$, alors l'action de G sur ses 2-Sylow induit un morphisme de groupe $\rho\colon G \to \mathfrak{S}_5$. Puisque G est simple et que ρ n'est pas trivial, alors ce morphisme est nécessairement injectif. Donc G s'identifie à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$. Un tel groupe G étant distingué dans $\mathfrak{S}_5$ c'est nécessairement $\mathfrak{A}_5$.
4. On suppose que $s_2 = 15$. Soient S_1 et S_2 deux 2-Sylow distincts. Alors $S_1 \cap S_2$ est un sous-groupe de S_2 donc est d'ordre 1 ou 2 (pas 4 puisque c'est un sous-groupe propre). Supposons que tous les 2-Sylow soient d'intersection triviale. Alors $|\cup_{i=1}^{15} S_i| = 3 \times 15 + 1 = 46$. Il existe donc 45 éléments d'ordre 2 ou 4 dans G, mais puisque $s_3 = 10$, il y a aussi $2 \times 10 = 20$ éléments d'ordre 3. C'est impossible puisque $45 + 20 > 60$.

   Donc il existe S_1 et S_2 des 2-Sylows vérifiant $S_1 \cap S_2 = \{1, g\}$.

   Par définition $C_G(g) = \{x \in G \mid xg = gx\}$. Puisque $C_G(g)$ est un sous-groupe de G alors $|C_G(g)||60$. De plus, tout groupe d'ordre 4 est abélien, donc $S_1 \subset C_G(g)$, donc $4||C_G(g)|$. Finalement on a $|C_G(g)| \in \{12, 20, 60\}$. Or $|C_G(g)| \neq 60$ puisque sinon on aurait $g \in Z(G)$, ce qui est impossible puisque $Z(G) = \{e\}$ par simplicité de G.

   • Supposons que $|C_G(g)| = 20$. On considère l'action de G sur $G/C_G(g)$ (qui est de cardinal 3). Elle induit un morphisme de groupe $\rho\colon G \to \mathfrak{S}_3$. Pour des raisons de cardinalité, ce morphisme n'est pas injectif. Il n'est pas non plus égal à G. Donc son noyau est un sous-groupe distingué non trivial de G. Ce qui est absurde puisque G est simple.

- Supposons que $|C_G(g)| = 12$. Comme précédemment, on considère l'action de G sur $G/C_G(g)$ (qui est de cardinal 5). Elle induit un morphisme de groupe $\rho\colon G \to \mathfrak{S}_5$. Le noyau de ce morphisme n'est pas tout G. Donc ρ est injectif (sinon G aurait un sous-groupe distingué non trivial) et G s'identifie à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$. Or il n'y en a qu'un et c'est $\mathfrak{A}_5$. Cependant $\mathfrak{A}_5$ ne possède que cinq 2-Sylow. C'est absurde.

Donc $s_2 = 5$.

$\square$